Таким образом, общетеоретические и научно-практические вопросы правового регулирования использования и применения различных информационных технологий, информационных систем и ресурсов требуют пристального внимания.

Важным вопросом является обеспечение безопасности национального сегмента сети Интернет. В постановлении Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» регулируются основные положения информационной безопасности. Обращается внимание на обеспечение кибербезопасности национального сегмента сети Интернет в сфере не только предоставления информационных услуг, но и реализации прав граждан в информационной сфере, в том числе в области защиты личных данных и защиты личной жизни, гарантируемых Конституцией Республики Беларусь. Основной задачей информационной безопасности от несанкционированного доступа, использования, раскрытия, искажения, исследования, уничтожения информации является сбалансированная защита конфиденциальности информации. Компьютерная безопасность, как раздел общей информационной безопасности, отвечает за меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие устройства), а также компьютерных сетей, включая сеть Интернет.

Для обеспечения кибербезопасности национального сегмента сети Интернет осуществляется система мониторинга с формированием облачной платформы комплексных сервисов. О киберинцидентах оперативно сообщается уполномоченным государственным органам, операторам электросвязи и командам быстрого реагирования на компьютерные инциденты. Специалисты команд CERT (англ. Computer emergency response team) – «компьютерная группа реагирования на чрезвычайные ситуации» и CSIRT (англ. Computer security incident response team) – «команда компьютерной безопасности по реагированию на инциденты» – это специалисты и эксперты по компьютерной безопасности, занимающиеся сбором информации о киберинцидентах, их классификацией и нейтрализацией. Данные специалисты должны не только быть компетентными техническими компьютерными специалистами, но и обладать обширными юридическими знаниями. Для возбуждения уголовных, административных дел специалисты также должны обладать навыками грамотного юридического оформления протоколов оценки IP-адресов, времени доступа к ресурсам, действий поставщиков интернет-услуг, сведений об адресах, используемых для кибератак. Правильно юридически задокументированная компьютерная информация важна и для страхования киберрисков и услуг тестирования компьютерных систем. Следует всегда помнить о достижении и сохранении баланса между надежной идентификацией пользователей, регистрацией их действий и созданием условий для безопасного сбора, обработки, предоставления, хранения и распространения персональных данных в национальном сегменте сети Интернет.

Академия МВД Республики Беларусь понимает важность и значимость для государства специалистов такого уровня, поэтому на кафедре правовой информатики введена новая учебная дисциплина «Комплексная защита информации и противодействие киберпреступности». Целями изучения данной учебной дисциплины являются усвоение обучающимися приемов и методов комплексной защиты информации, основ противодействия киберпреступлениям, а также подготовка к выполнению задач по обнаружению и фиксации электронно-цифровых следов в контексте будущей профессиональной деятельности.

В рамках данной дисциплины, обучающиеся будут изучать следующие темы: «Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь», «Каналы утечки информации и безопасность информационных систем», «Аппаратное и программное обеспечение защищенных компьютерных систем», «Основы противодействия киберпреступности», «Электронные доказательства».

Обучающиеся овладеют важными навыками по подбору сведений, фактов и сведений для раскрытия и расследования различных видов преступлений и правонарушений, смогут использовать передовые цифровые технологии для формирования доказательственной базы и грамотного оформления уголовных и административных дел. Такие системы мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз будут обеспечивать информационную безопасность, что в свою очередь будет способствовать предотвращению преступлений в информационной сфере, предусмотренных Уголовным кодексом Республики Беларусь (преступлений против информационной безопасности (киберпреступлений) и иных преступлений, предметом или средством совершения которых являются информация, информационные системы и сети).

Учитывая, насколько важным для государства является формирование, совершенствование и реализация организационных, правовых, научно-технических, правоохранительных, экономических мер по обеспечению национальной безопасности в информационной сфере, специалисты, подготовленные на кафедре правовой информатики Академии МВД Республики Беларусь, будут обладать необходимым уровнем знаний, умений и и навыков, направленных на обеспечение информационной безопасности общества, поддержание такого уровня защищенности информационной сферы, который обеспечит реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.

УДК 343.985

И.А. Шаматульский

ТИПИЧНЫЕ СПОСОБЫ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА И НАПРАВЛЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОГО ПРОТИВОДЕЙСТВИЯ ИМ

Как отмечает В.Н. Долинин, способ совершения преступлений представляет собой систему объединенных замыслом действий преступника по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами и сопряженных с использованием соответствующих орудий, средств и приемов.

На наш взгляд, можно выделить следующие наиболее типичные способы совершения мошенничества и определить действия оперативного сотрудника по противодействию им.

1. Получение кредитов в банковских организациях в интересах третьих лиц за счет потерпевших.

При проведении проверки по таким фактам необходимо получить: заявление лица о совершенном преступлении; объяснение заявителя о причинах получения кредита в интересах мошенника, обстоятельствах передачи ему денег, условий возврата долга, оплаты кредита и др.; объяснения свидетелей (очевидцы, члены семьи, поручители и т. д.) о договоренностях и обстоятельствах получения кредита, обстоятельствах его передачи третьему лицу, о платежеспособности кредитополучателя, о возврате долга; банковские документы по кредиту (кредитное досье), в том числе сведения о предоставлении кредита и его неуплате, уведомления банка о необходимости оплаты кредита, а также о расходных операциях по кредитным средствам; судебные решения о взыскании с кредитополучателя долга по кредиту; сведения о проверке кредитополучателя на наличие судимости за совершение преступлений против собственности; сведения о других кредитополучателях в интересах мошенника; объяснения лица, в действиях которого содержатся признаки мошеннических действий; видеозаписи из банкоматов и банков, посредством и на территории которых происходило получение кредитных средств; сведения об имущественном положении и наличии судимости лица, в действиях которого содержатся признаки мошеннических действий; аналогичные материалы проверок, по которым принято решение об отказе в возбуждении уголовного дела. При необходимости могут быть назначены соответствующие экспертизы.

2. Приобретение телефонов (планшетов), бытовой техники в кредит и передача их мошенникам.

При проведении проверки по таким фактам необходимо получить: заявление лица о совершенном преступлении; объяснение заявителя о причинах приобретения имущества в интересах подозреваемого, обстоятельствах передачи имущества, условиях возврата долга и оплаты кредита (рассрочки); объяснения свидетелей (очевидцев) о договоренностях и обстоятельствах передачи имущества, приобретенного в кредит (рассрочку) третьему лицу, о платежеспособности кредитополучателя; объяснения лиц, приобретавших товар, купленный в рассрочку до ее окончательной выплаты; объяснения работников, оформлявших приобретение товара в кредит (рассрочку), на предмет выполнения ими обязанностей по проверке личности кредитополучателя; документы, подтверждающие факт заключения сделки в кредит (рассрочку), в том числе сведения о предоставлении кредита (рассрочки) и его неуплате; судебные решения о взыскании с кредитополучателя долга за неоплату товара, приобретенного в кредит (рассрочку); объяснения лица, в действиях которого содержатся признаки мошеннических действий; сведения о проверке кредитополучателя на наличие судимости за совершение преступлений против собственности; сведения о других кредитополучателях в интересах мошенника; видеозаписи, подтверждающие факт нахождения и общения кредитополучателя и мошенника на территории торговых объектов, банковских организаций; сведения операторов связи и интернет-провайдеров о регистрации в сетях, перемещении и использовании телефона (планшета); сведения об имущественном положении и наличии судимости лица, в действиях которого содержатся признаки мошеннических действий; аналогичные материалы проверок, по которым принято решение об отказе в возбуждении уголовного дела.

3. Мошенничество, связанное с оказанием услуг по приобретению товара, перечислением денежных средств неизвестным пользователям, блокированием операционных систем (программ) под предлогом оплаты штрафа и последующей разблокировки, совершенное с использованием сети Интернет либо иной сети электросвязи общего пользования.

В данном случае сведения о лице, совершившем преступление, как правило, отсутствуют. При проведении проверки по таким фактам необходимо получить заявление лица о совершенном преступлении; объяснение лица, в отношении которого совершены противоправные действия, об обстоятельствах происшедшего с выяснением вопросов о размере причиненного вреда, обстоятельствах, при которых стало возможным общение с подозреваемым, перечисление денег и т. д.; сведения интернет-провайдера о пользователе услуг. Для установления IP-адресов, между которыми велась переписка, необходимо провести осмотр компьютера, к которому целесообразно привлечь специалиста; получить сведения об электронных адресах интересующих почтовых ящиков, фактах распространения вредоносных программ, блокирующих компьютер потерпевших, и др.; сведения о телефонных соединениях у соответствующего оператора связи; сведения о перечислении потерпевшим электронных денег. При наличии таких фактов следует устанавливать пользователей электронных кошельков (данные лица при регистрации; IP-адреса входов и выходов в учетную запись кошелька; сведения об операциях, совершенных с использованием всех имеющихся электронных кошельков, прикрепленных к идентификатору пользователя с момента его регистрации до исполнения запроса; информация о принадлежности и соединениях абонентских номеров операторов мобильной связи; установочные данные лица, указанные при регистрации почтовых ящиков, включая информацию о резервных ящиках, контрольном вопросе и ответе на него, времени регистрации ящика с указанием IP-адреса, с которого проводилась регистрация); сведения об имущественном положении и судимости лица, в действиях которого содержатся признаки преступления, при его установлении; аналогичные материалы проверок, по которым принято решение об отказе в возбуждении уголовного дела.

4. Мошенничество в сфере оказания услуг по реализации, подбору и приобретению автотранспорта.

При проведении проверки по таким фактам необходимо получить: заявление лица о совершенном преступлении и его объяснение об обстоятельствах передачи транспортного средства мошенникам, достигнутых с ними договоренностях, лицах, принимавших автомобиль на комиссию, и т. д. При этом также следует принять меры, направленные на определение стоимости похищенного транспорта и размера причиненного ущерба; все имеющиеся документы, касающиеся проведения сделки, как со стороны потерпевшего, так и со стороны организации, оказывавшей услуги по реализации, подбору и приобретению автотранспорта; сведения из органов судебной власти о заявленных потерпевшими исках и результатах их рассмотрения; сведения о перепродаже (передаче) автомобиля потерпевшего по более низкой цене иным лицам; сведения о регистрации субъекта хозяйствования, занимающегося оказанием услуг по комиссионной продаже автотранспорта; объяснения лица, в действиях которого содержатся признаки мошеннических действий, сведения о его судимости и имущественном положении; сведения обо всех лицах, потерпевших от действий мошенников, их объяснения. Следует также принять меры к исключению фактов переоформления спорного автотранспорта, при необходимости назначить соответствующие экспертизы.

Таким образом, целенаправленное противодействие мошенничеству невозможно без знания сотрудниками оперативных подразделений органов внутренних дел типичных способов совершения рассматриваемого вида преступлений.